

Appendix B, Attachment 1

FACILITY SECURITY STANDARDS CHART

M - MINIMUM STANDARD

S - STANDARD BASED ON FACILITY EVALUATION

D – DESIRABLE

N/A - NOT APPLICABLE

FACILITY LEVEL	I	II	III	IV
SECURITY PERSONNEL
FACILITY SECURITY PERSONNEL
Posts at all accessible entrances/exits	N/A	D	S	M
Roving Patrols	N/A	D	S	M
Armed Officers at all Magnetometer Screening Checkpoints	M	M	M	M
24 Hour Presence	N/A	D	M	M
Access to EOD K-9 Unit on a 24 Hour Basis	D	D	D	M
Designated Counter Surveillance Unit	N/A	N/A	D	S
Reliable 24 Hour Communication System for All Security Personnel	D	D	S	M
Interoperable Communications System With Other Organizations	D	D	D	S
Fixed Posts with 360 Degree Coverage	N/A	N/A	D	S
Dedicated Armed Security Presence	N/A	D	D	M
Dedicated Trained On Site Security Manager	N/A	D	D	S
OTHER LAW ENFORCEMENT IN FACILITY
Name, Contacts and Working Hours of Other Law Enforcement in the Facility	M	M	M	M
PERIMETER SECURITY
Secure Exterior Utility Systems, HVAC Systems, and Vulnerable Fuel Sources	N/A	D	S	M
PARKING
Control of Facility Parking	D	D	M	M
Control of Adjacent Parking (If Achievable)	D	D	D	S
Screen All Vehicles Within 100 Feet (If Achievable)	D	D	D	S
Avoid Leases Where Parking Cannot be Controlled	D	D	D	S
Post Signs and Arrange for Towing Unauthorized Vehicles	S	S	M	M
ID System and Procedures for Authorized Parking (Placard, Decal, Card Key, etc.)	D	D	M	M
Adequate Lighting for Parking Areas	D	S	M	M
Employee Parking Separated From Public Parking (If Achievable)	D	D	S	M

Bollards (other barriers) Preventing Unauthorized Access	D	D	D	M
CLOSED CIRCUIT TELEVISION (CCTV) MONITORING
CCTV Surveillance Cameras With Time Lapse Video Recording, Pan Tilt and Zoom Capability, Still Picture Capability, 360 Degree Coverage, with a Back-up Power Supply	D	S	S	M
Security Room with Two Officers Monitoring the CCTV System on a 24-Hour Basis	D	D	S	M
One Monitor for Every Eight Cameras	D	D	D	D
LIGHTING
Exterior Lighting with 360 Degree Coverage Around the Facility	S	S	S	M
Parking Area Lighting	D	D	D	S
Exterior/Interior Lighting with Emergency Power Backup	M	M	M	M
Lighting Meets Minimum for the CCTV System	M	M	M	M
PHYSICAL BARRIERS
Extend Physical Perimeter with Rated or Landscape Barriers (If Achievable)	N/A	N/A	D	S
Rated or Landscape Barriers Separating Drop Off/Parking Area from the Facility	N/A	N/A	D	S
ENTRY SECURITY
RECEIVING/SHIPPING
Review/Implement Receiving/Shipping Procedures	M	M	M	M
Restrict Delivery Access to Authorized Personnel/Vehicles	D	D	S	M
Post, Monitor or Secure Receiving/Shipping Areas	D	D	S	M
X-Ray All Incoming Packages	D	D	S	M
Irradiate All Incoming Mail	D	D	S	S
Security Training for Mailroom Personnel	D	D	S	M
ACCESS CONTROL
Card Key or Similar System to Record Entry/Exit Times	D	D	S	S
Security Personnel Posted at all Open Access Points Checking Identification	D	D	S	M
Intrusion Detection System (IDS) with 24-Hour Central Monitoring Capability	D	S	M	M
IDS Utilizing Line Supervision and Backup Power	D	D	S	M
IDS Covering all Access Points	D	S	S	M
Central Database Containing the Location and Serial Number of all Keys	S	S	S	M
ENTRANCES/EXITS
X-Ray and Magnetometer at Public Entrances with Trained Operators	N/A	D	S	M
Require X-Ray Screening of All Packages	N/A	D	S	M

Radiation Screening Device	N/A	D	D	S
Peep Holes	S	S	N/A	N/A
Intercom	S	S	N/A	N/A
Entry Control w/CCTV and Door Strikes	D	S	N/A	N/A
Post Signs Advising of 24 Hour Video Surveillance (if CCTV system in use)	M	M	M	M
High Security Locks	M	M	M	M
Door Hinges Located on the Inside	M	M	M	M
Secure Doors/Set Alarms on Off Hours	M	M	M	M
INTERIOR SECURITY
EMPLOYEE/VISITOR IDENTIFICATION
Agency Photo ID for all Personnel Displayed at all Times	N/A	D	S	M
Visitor Control System	D	M	M	M
Visitor Identification Accountability System	N/A	D	S	M
Establish Identification Issuing Authority	S	S	S	M
UTILITIES – INCLUDING HVAC
Prevent Unauthorized Access to Utility Areas	S	S	M	M
Provide Emergency Power to Critical Systems (Alarm Systems, Radio Communications, Computer Facilities, etc.)	M	M	M	M
Ability and Procedures to Close Air Intake System	D	D	S	S
Dedicated HVAC systems for lobbies, mailrooms, and loading docks	D	D	D	S
OCCUPANT EMERGENCY PLANS
Examine, Update and Practice Occupant Emergency Plans (OEP) and Contingency Procedures Based On Threats	M	M	M	M
Contacts for Local Police, Fire Department, HAZMAT Teams, EOD Team, etc.	M	M	M	M
Assign and Train OEP Officials (Assignment Based on Largest Tenant in the Facility)	M	M	M	M
Annual Tenant Training	M	M	M	M
Establish Relocation Primary and Secondary Sites	M	M	M	M
DAYCARE CENTERS
Evaluate Whether to Locate Daycare Centers in Federal Facilities	N/A	M	M	M
Review Location, Access, Evacuation, Drop-off/Pick-up Procedures Once Per Year	N/A	M	M	M
CYBER ISSUES
All Official Computers in Compliance with Current DOI Security Standards	M	M	M	M
“Stand Alone” Computers in Control of Vital Systems	D	D	D	D
Back-up Power Supply for Computers Monitoring Security/Vital Systems	D	D	S	M
FIRE RESCUE/LIFE SAFETY

Appendix B, Attachment 2

DETAILS OF RECOMMENDED SECURITY STANDARDS

Security Personnel	
Term	Definition/Description
FACILITY SECURITY PERSONNEL
POSTS AT ALL ENTRANCES/EXITS	All accessible entrance/exits, will have stationed security personnel adhering to entrance/exit protocol.
SECURITY FIXED POST	A fixed area of responsibility designated for observation, screening or performing information gathering by security personnel. Security personnel will only deviate from this location when they are relieved or in a critical emergency situation (i.e. fire, etc.).
ROVING PATROLS	Geographic areas designated for general observation, response or performing information gathering by security personnel. Security personnel will only deviate from the patrol area when they are relieved or in a critical situation.
ARMED OFFICERS AT ALL MAGNETOMETER SCREENING CHECK POINTS	A percentage of the security force should be authorized to carry firearms. At a minimum, these personnel should be positioned at all screening areas, on roving patrols, and in the response mode.
24-HOUR PRESENCE	The security force should maintain a constant presence at the facility.
ACCESS TO EOD K-9 UNIT ON A 24-HOUR BASIS	Ability to contact and summon an explosive ordinance division dog to assist in suspicious package identification.
COUNTER SURVEILLANCE UNIT	Security personnel in an “under-cover” roving patrol observing possible vulnerabilities and gathering information. The personnel remain in contact with the control room and only respond and identify themselves in exigent circumstances.
RELIABLE 24-HOUR COMMUNICATION SYSTEM	A communication system issued to all security personnel with a minimal amount of “dead” spots that is monitored on a 24-hour basis.
INTEROPERABLE COMMUNICATION	A reliable 24-hour communications system

Security Personnel	
SYSTEM WITH OTHER ORGANIZATIONS	that can be monitored/used by other law enforcement organizations.
360 DEGREE COVERAGE	Security posts positioned to effectively eliminate any non-screened/observed individual from entering a secure area.
DEDICATED TRAINED ON SITE SECURITY MANAGER	A Security Manager who has completed Security Training at FLETC or other accredited Security Managers Course.
OTHER LAW ENFORCEMENT IN FACILITY
NAME, CONTACTS, AND WORKING HOURS OF OTHER LAW ENFORCEMENT IN FACILITY	Maintain liaison contact for intelligence issues, emergency response, etc.

Perimeter Security	
Term	Definition/Description
PARKING
SECURE EXTERIOR UTILITY SYSTEMS, HVAC SYSTEMS, AND VULNERABLE FUEL SOURCES	Exterior utility systems should be assessed for possible vulnerabilities and appropriate measures should be taken.
CONTROL OF FACILITY PARKING	Access to government parking should be limited where possible to government vehicles and personnel. At a minimum, authorized parking spaces and vehicles should be assigned and identified.
CONTROL OF ADJACENT PARKING	Where feasible, parking areas adjacent to Federal space should also be controlled to reduce the potential for threats against Federal facilities and employee exposure to criminal activity.
SCREEN ALL VEHICLES WITHIN 100 FEET	All vehicles entering a perimeter of 100 feet of the facility should be visually or K-9 searched.
AVOID LEASES WHERE PARKING CANNOT BE CONTROLLED	Endeavor to negotiate guard services as part of the lease.
POST SIGNS AND ARRANGE FOR TOWING UNAUTHORIZED VEHICLES	Procedures should be established and implemented to alert the public to towing policies and the removal of unauthorized vehicles.
ID SYSTEM AND PROCEDURES FOR AUTHORIZED PARKING	Procedures should be established for identifying vehicles and corresponding parking spaces. (Placard, decal, card key, etc.)

Perimeter Security	
ADEQUATE LIGHTING FOR PARKING AREAS	Effective lighting provides added safety for employees and deters illegal or threatening activities.
EMPLOYEE PARKING SEPERATED FROM PUBLIC PARKING	Segregating the parking allows for different levels of screening.
BOLLARDS PREVENTING UNAUTHORIZED ACCESS	Barriers (bollards, landscaping, etc.) should be strategically positioned around the facility to increase the standoff distance of unauthorized vehicles.
CLOSED CIRCUIT TELEVISION (CCTV) MONITORING
CCTV SURVEILLANCE CAMERAS WITH TIME LAPSE VIDEO RECORDING, PTZ CAPABILITY, STILL PICTURE CAPABILITY, 360 DEGREE COVERAGE, WITH A BACK-UP POWER SUPPLY	Twenty-four hour CCTV surveillance and recording is desirable at all locations as a deterrent. Requirements will depend on assessment of the security level for each facility. Time-lapse video recordings/still pictures are also highly valuable as a source of evidence and investigative leads.
SECURITY ROOM WITH TWO OFFICERS MONITORING THE CCTV SYSTEM ON A 24-HOUR BASIS	Security cameras have been used to decrease the manpower needed in certain areas. Cameras are only effective when they are being monitored.
ONE MONITOR FOR EVERY EIGHT CAMERAS	Eight is about the maximum number of cameras that can effectively cycle through one monitor.
LIGHTING
EXTERNAL LIGHTING WITH 360 DEGREE COVERAGE	All attempts should be made to minimize any “dark” spots near or adjacent to any facility.
PARKING AREA LIGHTING	Employee parking areas require adequate illumination.
EXTERIOR/INTERIOR LIGHTING WITH EMERGENCY POWER BACKUP	Standard safety code requirement in virtually all areas. Provides for safe evacuation of facilities in case of natural disaster, power outage or criminal/terrorist activity.
LIGHTING MEETS MINIMUM FOR THE CCTV SYSTEM	The CCTV monitoring system will not be effective without proper illumination.
PHYSICAL BARRIERS
EXTEND PHYSICAL PERIMETER WITH RATED OR LANDSCAPE BARRIERS (IF ACHIEVABLE)	This security measure will only be possible in locations where the Government controls the property and where physical constraints are not present. (Barriers of concrete, steel, trees, boulders, earthen walls, etc.)

Perimeter Security	
RATED OR LANDSCAPE BARRIERS SEPARATING DROP OFF/PARKING AREA FROM FACILITY	Desirable to prevent unauthorized vehicle access into the parking area and from the parking area to the facility.

Entry Security	
Term	Definition/Description
RECEIVING/SHIPPING
REVIEW/IMPLEMENT RECEIVING/SHIPPING PROCEDURES	Audit current standards for package entry, suggest ways to enhance security, and implement improved procedures.
RESTRICT DELIVERY ACCESS TO AUTHORIZED PERSONNEL/VEHICLES	Unauthorized passenger or other vehicles should not be allowed access to park, drop-off passengers or “stand” in the loading area.
POST, MONITOR OR SECURE RECEIVING/SHIPPING AREAS	See “Security Post” and “CCTV” definitions. Secure (lock) the area when not in use.
X-RAY ALL INCOMING PACKAGES	In an attempt to detect an explosive, incendiary device, weapon, etc.
IRRADIATE ALL INCOMING MAIL	In an attempt to render safe a biological devise
SECURITY TRAINING FOR MAILROOM PERSONNEL	All Mailroom personnel should have yearly training regarding the detection and mitigation of hazardous substances/devices.
ACCESS CONTROL
CARD KEY OR SIMILAR SYSTEM TO RECORD ENTRY/EXIT TIMES	Prevents unauthorized entry and keeps a current database of who is located in the facility and usage of the facility on different days and times.
SECURITY GUARD POSTED AT ALL OPEN ACCESS POINTS CHECKING IDENTIFICATION	See “Security Post.”
INTRUSION DETECTION SYSTEM (IDS) WITH 24-HOUR CENTRAL MONITORING CAPABILITY	A basic, cost effective security measure.
IDS USING LINE SUPERVISION AND BACKUP POWER	An IDS system that is activated if the main reporting line is interrupted (i.e. phone line is cut) and is not affected by power fluctuations.
IDS COVERING ALL ACCESS POINTS	All possible entrances/exits into the facility should be covered by this system, not just key locations.
CENTRAL DATABASE CONTAINING	The integrity of the locking system must be

Entry Security	
THE LOCATION AND SERIAL NUMBER OF ALL KEYS	maintained.
ENTRANCES/EXITS
X-RAY AND MAGNETOMETER AT PUBLIC ENTRANCES WITH TRAINED OPERATORS	These devices, although an excellent visual deterrent, will only be truly effective if operated by trained personnel.
REQUIRE X-RAY SCREENING OF ALL MAIL/PACKAGES	All packages entering facility should be subject to x-ray screening and/or visual inspection.
RADIATION SCREENING	For use in level IV and Critical Infrastructures/Key Asset facilities.
PEEP HOLES	Easy and effective visual recognition system for small offices.
INTERCOM	Communication tool that can be used in combination with peephole.
ENTRY CONTROL WITH CCTV AND DOOR STRIKES	Provides employees with the ability to view and communicate remotely with visitors before allowing access. Not applicable for facilities requiring screening devices.
POST SIGNS ADVISING OF 24-HOUR VIDEO SURVEILLANCE	Warning signs advising of 24-hours surveillance act as a deterrent in protecting employees and facilities.
HIGH SECURITY LOCKS	Any exterior entrance should have a high security lock as determined by FPS specifications and/or agency requirements.
DOOR HINGES LOCATED ON THE INSIDE	Basic security measure.
SECURE DOORS/SET ALARMS ON DURING SECURE HOURS	Any security system is ineffective if not operated properly.

Interior Security	
Term	Definition/Description
EMPLOYEE/VISITOR IDENTIFICATION
AGENCY PHOTO ID FOR ALL	May not be required in smaller facilities.

Interior Security	
PERSONNEL DISPLAYED AT ALL TIMES	
VISITOR CONTROL/SCREENING SYSTEM	Facilities should develop a method to have visitors sign-in and may require an escort or formal identification/badge.
VISITOR ID ACCOUNTABILITY SYSTEM	Stringent methods of control over visitor badges will ensure that visitors wearing badges have been screened and are authorized to be at the facility during the appropriate time frame.
ESTABLISH ID ISSUING AUTHORITY	Develop procedures and establish authority for issuing employee and visitor IDs.
UTILITIES
PREVENT UNAUTHORIZED ACCESS TO UTILITY AREAS	Smaller facilities may not have control over utility access, or locations of utility areas. Where possible, assure utility areas are secure and only authorized personnel can gain entry.
PROVIDE EMERGENCY POWER TO CRITICAL SYSTEMS	Tenant agency is responsible for determining which computer and communication systems require back-up power. All alarm systems, CCTV monitoring devices, fire detection systems, entry control devices, etc., require emergency power sources.
ABILITY AND PROCEDURES TO CLOSE AIR INTAKE SYSTEM	Essential to a “shelter in place” plan. Facility Managers should assess and decrease the vulnerability of their facility HVAC system against a Chemical, Biological, and Radiological (CBR) threat.
DEDICATED HVAC SYSTEMS FOR LOBBIES, MAILROOMS. AND LOADING DOCKS	Separate HVAC systems will prevent the contamination of one vulnerable area being spread throughout other areas in the facility.
OCCUPANT EMERGENCY PLANS
EXAMINE OCCUPANT EMERGENCY PLAN (OEP) AND CONTINGENCY PROCEDURES BASED ON THREATS	Review and update current OEP procedures for thoroughness. OEP’s should reflect the current security climate.
CONTACTS FOR LOCAL POLICE, FIRE DEPARTMENT, HAZMAT TEAMS, EOD TEAM, ETC.	Contact list should be kept in an accessible area and updated once per year.
ASSIGN AND TRAIN OEP OFFICIALS	Assignment based on GSA requirement that

Interior Security	
	largest tenant in facility maintain OEP responsibility. DOI officials should be assigned, trained, and contingency plan established to provide for the possible absence of OEP officials in the event of emergency activation of the OEP.
ANNUAL TENANT TRAINING	All tenants should be aware of their individual responsibilities in an emergency situation.
ESTABLISH RELOCATION PRIMARY AND SECONDARY SITES	All tenants should be aware of the relocation sites.
DAY CARE CENTERS
EVALUATE WHETHER TO LOCATE DAYCARE CENTERS IN LEVEL III AND IV FACILITIES	Conduct a thorough review of security and safety standards.
REVIEW LOCATION, ACCESS, EVACUTION, DROP-OFF/PICK-UP PROCEDURES ONCE PER YEAR	Daycare Centers should be included in all security assessments.
CYBER ISSUES
ALL OFFICIAL COMPUTERS IN COMPLIANCE WITH CURRENT DOI SECURITY STANDARDS	The CIO's Office should be contacted with any questions/concerns.
"STAND ALONE" COMPUTERS IN CONTROL OF VITAL SYSTEMS	Computers that are not connected to outside systems, i.e. the internet, other DOI systems, etc.
BACK-UP POWER SUPPLY FOR COMPUTERS MONITORING SECURITY/VITAL SYSTEMS	In an effort to negate the power supply as a vulnerability.
FIRE RESCUE/LIFE SAFETY
PRESENCE OF A FACILITY EMERGENCY PUBLIC ADDRESS SYSTEM	A communication system used to transmit emergency information to facility occupants.
ESTABLISH "SHELTER IN PLACE" PLAN	Determine if the facility is acceptable for use during an emergency.

Security Planning	
Term	Definition/Description
INTELLIGENCE SHARING
ESTABLISH A SECURITY LIASION	At least one Officer should be the liaison

Security Planning	
OFFICER	contact for other law enforcement agencies. This Officer will be responsible for updating liaison contacts, attending meetings, disseminating information, etc.
REVIEW/ESTABLISH PROCEDURES FOR INTELLIGENCE RECEIPT/DISSEMINATION	Determine what procedures exist to ensure timely delivery and dissemination of critical intelligence. Review and improve procedures to alert agencies and specific targets of criminal and terrorist threats. Establish standard administrative procedures for response to incoming alerts.
ESTABLISH "IN-OFFICE" UNUSUAL FACILITY INCIDENT REPORTING SYSTEM	Provides an historical document for detecting patterns, official record of prior incidents, etc.
TRAINING
CONDUCT ANNUAL SECURITY AWARENESS TRAINING (INCLUDING CHEMICAL/BIOLOGICAL/RADIOLOGICAL)	Provide security awareness training for all tenants. At a minimum, self-study programs utilizing videos and literature, etc. should be implemented. These materials should provide up-to-date information covering security practices, employee security awareness, and personal safety.
ESTABLISH STANDARDIZED ARMED AND UNARMED GUARD QUALIFICATIONS/TRAINING REQUIREMENTS	Requirements for these positions should be stringently followed.
TENANT ASSIGNMENT
CO-LOCATE AGENCIES WITH SIMILAR SECURITY NEEDS	To capitalize on efficiencies and economies, agencies with like security requirements should be located in the same facility if possible.
DO NOT CO-LOCATE HIGH/LOW RISK AGENCIES	Low risk agencies should not take on additional risk by being located with high risk agencies.
ADMINISTRATIVE PROCEDURES
REVIEW GUIDELINES TO ESTABLISH FLEXIBLE WORK SCHEDULE IN HIGH THREAT/HIGH RISK AREA TO MINIMIZED EMPLOYEE VULNERABILITY TO CRIMINAL ACTIVITY.	Flexible work schedules can enhance employee safety by staggering reporting and departure times. As an example, flexible schedules might enable employees to park closer to the facility by reducing the demand for parking at peak times of the day.
ARRANGE FOR EMPLOYEE PARKING IN/NEAR FACILITY AFTER NORMAL	Minimize exposure to criminal activity by allowing employees to park at or inside the

Security Planning	
WORK HOURS	facility.
ESTABLISH SECURITY CONTROL PROCEDURES FOR SERVICE CONTRACT PERSONNEL	Establish procedures to ensure security where private contract personnel are concerned. Procedures may be as simple as observation or could include sign-in/escort. Frequent visitors may necessitate a background check with contractor ID issued.
CONSTRUCTION/RENOVATION
INSTALL MYLAR FILM ON EXTERIOR WINDOWS (SHATTER PROTECTION)	Application of shatter resistant material to protect personnel and citizens from the hazards of flying glass as a result of impact or explosion.
REVIEW CURRENT PROJECTS FOR BLAST/NATURAL DISASTER STANDARDS	Design and construction projects should be reviewed if possible, to incorporate current technology and blast standards. Immediate review of ongoing projects may generate savings in the implementation of upgrading to higher blast standards prior to completion of construction.
REVIEW/ESTABLISH UNIFORM STANDARDS FOR CONSTRUCTION	Review, establish, and implement uniform construction standards as it relates to security considerations.
REVIEW/ESTABLISH NEW DESIGN STANDARD FOR BLAST RESISTANCE	In smaller facilities or those that lease space, control over design standards may not be possible. However, future site selections should attempt to locate in facilities that do meet standards. New construction of Government controlled facilities should review, establish, and implement new design standards for blast resistance.
REVIEW APPROPRIATENESS OF INSTALLING VEHICLE BARRIERS	Barriers (various types) may need to be installed to increase “stand-off” distance from the facility.
ESTABLISH STREET SET-BACK FOR NEW CONSTRUCTION	Every foot between a potential bomb and a facility will dramatically reduce damage and increase the survival rate. Street setback is always desirable, but should be used in conjunction with barriers in Level IV facilities.
REVIEW CURRENT PROJECTS FOR FIRE SAFETY CODE	All new projects should be current with all safety codes.